Remarks

Claims 1-14, 16-22 are presented for the Examiner's review and consideration. Claims 1 and 17 have been amended and claim 15 has been cancelled. Applicants believe the claim amendments, cancellations, and the accompanying remarks herein serve to clarify the present invention and are independent of patentability. No new matter has been added.

35 U.S.C. §102 Rejection based on Ausubel

Claims 1-3, 5-9, 11, and 16-22 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 5,905,975 to Ausubel ("Ausubel"). For the reasons set forth below, Applicants respectfully submit that this rejection should be withdrawn.

Ausubel discloses a computer implemented system and method of executing an auction. (Abstract). Ausubel discloses, in one respect, a computerized system which allows flexible bidding by participants in a dynamic auction, combining some of the advantageous facets of the sealed-bid format with the basic advantages of an ascending-bid format. (Col. 1, lns. 61-65).

As illustrated in FIG. 1, the auction system includes an auctioneer's system 10 and a plurality of user systems 20, 30, and 40, each user system 20, 30, or 40 represents an individual bidder. (Col. 7, lns. 11-14). As is shown in FIG. 2, the auctioneer's system 10 implements a query process 18, a typical user system 20 implements a user process 28; the two processes also use message(s) 64 which are transmitted from the auctioneer's system 10 to a user system 20. (Col. 8, lns. 23-27). In response to a message from the auctioneer's system 10, the user process 28 may generate or modify flexible bid information 61 which is coupled to the database process 60. (Col. 8, lns. 28-31).

"Typically, an auction begins with a message transmitted from the auctioneer's system 10 to each user system 20, 30, etc. The user system allows (if needed—as will become clear below) the entry of flexible bid information to the database process 60. After the passage of sufficient time, allowing each of the user systems to enter whatever flexible bid information is necessary, the auctioneer's system 10 sends one or more queries to the database process for a particular user. The database process performs database look-ups for data relevant to the current questions, uses

the response to generate an answer, and sends the answer to the auctioneer's system 10. The database process may perform calculations and/or logical operations in generating the answers. The auctioneer's system 10 may then generate queries to the database process for other users. After answers are received from some or all of the users, the auctioneer's system 10 can perform calculations and/or logical operations to compute additional questions, allow the auctioneer to enter data, compute additional messages to be sent to the user systems, etc. Depending upon the particular auction involved and the answers, the auctioneer's system may conclude that the auction has been concluded and send a final message to one or more of the user systems." (Col. 8, ln. 58 – col. 9, ln. 13).

At any point in the auction, bidders are provided the opportunity to submit not only their current bids, but also to enter future bids (to be more precise, bidding rules which may have the opportunity to become relevant at future times or prices), into the auction system's database. (Col. 1, ln. 65 – col. 2-ln. 3). Moreover, participants are continually provided the opportunity to revise their bids associated with all future times or prices which have not already been reached, by entering new bids which have the effect of superseding this bidder's bids currently residing in the auction system's database. (Col. 2, lns.3-8).

In example six of Ausubel, the process or subroutine above entitled "Two-User Auction for Multiple Dissimilar Objects" may be used not only as a subroutine for the querying of participants in an auction, but also as a subroutine which improves the efficiency of calculations within an auction. (Col. 25, lns. 59-63). At the same time, the output of this subroutine may usefully be provided to auction participants as a means of justifying the auction outcome to them without unnecessarily disclosing the actual bids of other participants. (Col. 25, lns. 63-67). This may be especially useful in situations where the auctioneer can be trusted to maintain the privacy of bid information, but where it is more likely that participants can be induced to bid their true values if disclosure to rival bidders can be avoided. (Col. 25, ln. 67- col. 26, lns 4).

FIG. 7 illustrates one embodiment of an auction where users submit bids for subsets of the available units and the auctioneer discloses the minimal information to justify the auction outcome. (Col. 26, lns. 21-24). The final message(s) may include part or all of the results of the auction, namely that for each $i \in \{1, \ldots, n\}$, subset S_i has been assigned to user i, and at a price of

P_i. (Col. 27, lns. 1-4). Optionally, at step 711 the final message to user i may include the results of all the subauctions of user i versus "composite user"-i for set Ω, executed in the subroutine call at step 707. (Col. 26, lns. 19-24). (Col. 27, lns. 14-7). It is precisely the results of these subauctions which constitute the minimal information needed to justify the auction results to user i. (Col. 27, lns.79). The user system(s) which receive final message(s) will preferably display that information for the benefit of the user(s). Col. 27, lns.9-11).

As such, Ausubel discloses an auction system utilizing an auctioneer's system and a plurality of individual user systems in communication with the auctioneer's system. An auction begins with a message transmitted from the auctioneer's system to each user systems. At any point in the auction, the users are provided the opportunity to submit not only their current bids, but also to enter future bids. During the bidding process the auctioneer will query the users, and can provide minimal information, not including other users' bids, which can induce bidders to bid their true value of the item. Upon completion of the auction, the auctioneer can send to the users' information to justify the auction results, which can include results of the auction and the results of the all of the subauctions versus a composite user. However, Ausubel fails to disclose the publishing by the auctioneer to each of the users a function and a proof for that function, which can be verified by each of the user to verify that an auction results.

In contrast, the apparatus and method of the present invention comprises an auction service that is used in a network, such as, the Internet, and uses clients and/or servers. (Page 4, lns. 28-31). The goal of a protocol is to aggregate the preferences of the parties in order to decide on some social choice (for example, to decide whether a community should build a bridge, or how to route packets in a network, or to decide who wins an auction). (Page 5, lns. 21-24). Each party has a utility function which expresses how much that party values each possible outcome of the protocol (the bid in an auction, for example, is such a utility function). (Page 5, lns. 24-26). Each party sends information about its utility function to a center, which decides on the outcome of the protocol based on the reports from the parties, according to a specified function of the utility functions (for example, in a sealed-bid auction, the specified function that determines the winner is the maximum of the bids). (Page 5, lns. 26-30). The present invention is a method, system and apparatus that enables the center to compute and publish the output of F and to prove

to all parties that it computed F correctly. (Page 3, lns. 23-25). This is done without revealing the value of the input of a party to any other party. (Page 3, lns. 25-26).

In the case of auctions, the center is the auctioneer. (Page 7, ln. 18). It publishes the auction, receives the bids from the bidders, and computes the outcome of the auction. (Page 7, lns. 18-20). "The Steps include the following sequence. (1) The center announces the computation and commits to the circuits. (2) Party 1 sends a commitment to its input (Party 1 represents a generic party, and this operation is performed by each of the participating parties). (3) The center publishes the commitments. (4) Party 1 opens its commitment, and the center verifies it. (5) The center computes the function. (6) The center publishes a proof that the computation was correct, and Party 1 verifies it." (Page 7, ln. 25-page8, ln. 2).

As such, the present invention discloses an auction system which computes an output for a function F. The function F is computed is based on the inputs of the users. The system provides the output for the function F to the users, as well as a proof of the correctness of the output calculation. Ausubel fails to disclose calculating and providing an output for a function F to each user and providing a proof of correctness of the output to each user, which each user can verify the function F. Ausubel only discloses the sending of information to the users which can only justify the auction results, no verification protocol is provided. Further, the present invention does not query the users to induce the user to bid a true value, which is an important aspect of Ausubel.

Independent claim 1 recites, *in part*, computing and publishing a function F(X.sub.1,X.sub.2,...,X.sub.n) by the center A based on the input messages it receives, including generating a proof that the correct output of the function F(X.sub.1,X.sub.2,...,X.sub.n) was computed and publishing by center A to each of the users additional information which lets each of the users verify that F was computed correctly, and preventing a coalition of any one subset of the users from learning (i) anything which cannot be computed just from the output of the function, F(X.sub.1,...,X.sub.n), and from their own inputs, and (ii) information about the inputs of other users. Independent claim 17 includes analogous elements.

In light of the foregoing, independent claim 1 is respectfully submitted to be patentable over Ausubel. As claims 2-3, 5-9, 11, and 16 depend from claim 1 and claims 18-22 depend

from claim 17, these dependent claims necessarily include all the elements of their base claim. Accordingly, Applicants respectfully submit that the dependent claims are allowable over Ausubel at least for the same reasons.

35 U.S.C. §103 Rejections

Claim 10 was rejected under 35 U.S.C. 103(a) as being unpatentable over Ausubel in view of U.S. Patent No. 6,285,989 to Shoham ("Shoham"). Claims 4, 8, and 12-14 were rejected under 35 U.S.C. 103(a) as being unpatentable over Ausubel in view of U.S. Patent No. 6,021,398 to Ausubel ("'398 patent"). Claims 4, 8, 10, and 12-15 depend from claim 1. As noted above claim 1 is patentable over Ausubel. The inclusion of Shoham and the '398 patent fails to overcome the deficiencies in Ausubel. Accordingly, Applicants respectfully submit that the dependent claims are allowable at least for the same reasons.

Claim 15 was rejected under 35 U.S.C. 103(a) as being unpatentable over Ausubel in view of U.S. Patent No. 6,055,508 to Naor et al. ("Naor").

Initially, Applicants note that claim 15 has been canceled rendering the rejection of this claim moot. However, claim 1 has been amended to include the elements of claim 15.

The Examiner states that Ausubel also teach the Universal Surveillance Console (USC) which allows a third party to monitor the integrity of the operation (Col. 11,lns 1-20).

However, Applicants submit, that Ausubel does not disclose a USC nor any other device which allows a third party to monitor the integrity of the operation and that (Col. 11, lns. 1-20) are unrelated to such. Accordingly, Applicants submit that the combination of Ausubel and Naor fails to disclose the elements of claim 1.

In light of the foregoing, independent claim 1 is respectfully submitted to be patentable over Ausubel in view of Naor.

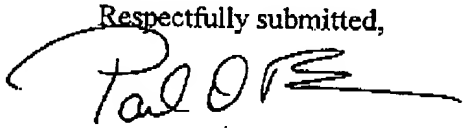
Conclusion

In light of the foregoing remarks, this application is now in condition for allowance and early passage of this case to issue is respectfully requested. If any questions remain regarding this amendment or the application in general, a telephone call to the undersigned would be

appreciated since this should expedite the prosecution of the application for all concerned.

No fee is believed to be due. However, please charge any required fee (or credit any overpayments of fees) to the Deposit Account of the undersigned, Account No. 500601 (Docket No. 704-X00-047US).

Respectfully submitted,



Martin Fleit, Reg. # 16,900
Paul Bianco, Reg. # 43,500

Customer Number: 27317
Martin Fleit
FLEIT KAIN GIBBONS GUTMAN BONGINI & BIANCO, P.L.
21355 East Dixie Highway, Suite 115
Miami, Florida 33180
Tel: 305-830-2600; Fax: 305-830-2605
e-mail: mfleit@fleitkain.com